UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/505,951 | 02/15/2000 | Simon Robert Walmsley | AUTH08US | 5608 |

7590 08/17/2006

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

| EXAMINER | |
|---|---|
| DAVIS, ZACHARY A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

DATE MAILED: 08/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/505,951 | WALMSLEY ET AL. | |
| | Examiner | Art Unit | |
| | Zachary A. Davis | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *08 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,2,4-14 and 16-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-14 and 16-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20060608*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08 June 2006 has been entered.

2. By the above submission, Claims 1 and 11 have been amended. Claims 3 and 15 have been canceled. No new claims have been added. Claims 1, 2, 4-14, and 16-20 are currently pending in the present application.

### *Response to Arguments*

3. Applicant's arguments filed 08 June 2006 have been fully considered but they are not persuasive.

Claims 1, 2, 4, 6-14, and 17-20 were rejected under 35 U.S.C. 103(a) as unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Spies et al, US Patent 5689565. Claims 5 and 16 were rejected under 35 U.S.C.

103(a) as unpatentable over Sony in view of Spies and further in view of Schneier, *Applied Cryptography*.

The Examiner notes that, again, Applicant's response is not considered to be fully responsive under 37 CFR 1.111(b). Specifically, Applicant's reply must reply to every ground of objection and rejection in the previous Office action, and must present arguments pointing out the specific distinctions believed to render the claims, including any newly presented claims, patentable over any applied references. Applicant has not replied to the rejections of Claims 2, 4-14, or 16-20 under 35 U.S.C. 103(a) and has not presented any arguments specifically in reference to Claims 2, 4-14, or 16-20. However, given the dependences and the correspondence between the claims, the Examiner has considered the present response to be a *bona fide* attempt to advance the prosecution of the present application; therefore, the present response and the arguments therein have been considered as set forth below.

In reference to Claim 1, in response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Applicant further argues that "the combination of Sony and Spies fails to teach or suggest the claim limitation of comparing the signatures and in the event that the signatures match, encrypting the decrypted random number and returning it to the trusted authentication chip" (see page 8 of the present response). Applicant further argues that there is nothing in Sony to suggest that there is a condition that needs to be satisfied in order to pass the encrypted random number between the two chips (see page 7 of the present response) and that "Spies is silent with respect to the use of random numbers and only describes the use of randomly selected keys" (see page 7 of the present response). First, regarding the latter contention, the Examiner respectfully disagrees, noting that a random key is clearly also a random number. Further, regarding the broader argument that there is nothing to suggest a condition to be satisfied before passing the number between the chips, the Examiner again disagrees. Particularly, the Examiner believes that it would be inherent at least in the authentication protocol disclosed by Sony to stop the protocol if any particular step of verification failed. Therefore, the Examiner believes that upon incorporation of the signature verification as taught by Spies into the method of Sony, if that signature verification failed (i.e. the signatures did not match), then it would be inherent or at least obvious not to continue the protocol.

In response to applicant's argument that there is no motivation to combine the references (see page 8 of the present response), the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or

motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation would be as cited in the previous Office actions, namely to authenticate the sending of the random number (see Spies, column 13, lines 26-32) and more generally to allow for greater security, privacy, authenticity, and integrity in the system (see Spies, column 2, lines 1-4).

In reference to the features of canceled Claims 3 and 15 that have been added by amendment to Claims 1 and 11, Applicant argues that the cited portion of Sony (column 8, lines 12-15) does not disclose the trusted authentication chip having a random function to produce random numbers from a seed (see page 8 of the present response). Specifically, Applicant argues that the random numbers in Sony are generated in the untrusted component (because Sony discloses a method for mutual authentication), as opposed to being generated in the trusted component as claimed. However, the Examiner respectfully disagrees. The Examiner has previously noted that the mutual authentication of Sony is viewed as encompassing two simultaneous one-way authentication operations, and when the reader/writer is authenticating the IC card, the reader/writer must clearly trust itself, even if the IC card is untrusted (see the Advisory action mailed 26 April 2005). Therefore the Examiner believes that Sony discloses that the trusted chip does, in fact, generate the random number (see Sony, column 8, lines 12-17, as cited by Applicant on page 9 of the present response, where the reader/writer corresponds to the trusted chip). Applicant further argues that there is

no description in Sony of how random numbers are generated; however, the Examiner believes that it is well known in the art to generate random numbers using a random function that uses a seed.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

***Examiner's Note***

4. The Examiner notes the use of the pronoun "it" in Claim 1 at line 19 of the claim. This appears to refer back to the encrypted random number of line 18. The Examiner also notes the use in Claim 11 of "the decrypted one" at line 9 of the claim, which appears to refer back to the signature of line 7; the use in Claim 11 of "it" at line 10, which appears to refer back to the encrypted random number also of line 10; and the use also in Claim 11 of "it" at line 12, which appears to refer back to the encrypted version of the random number of lines 11-12. Although it is clear to what each of these pronouns refers, the Examiner reminds Applicant that care should be taken with the use of pronouns to ensure that their antecedents are clear, to avoid any issues of indefiniteness under 35 U.S.C. 112, second paragraph.

***Double Patenting***

5. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or

discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

6. Claims 4 and 11 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 3 and 15, respectively, of copending Application No. 10/203,559 (published as US Patent Application Publication 2003/0159036). This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

7. Claims 6 and 11 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 3 and 15, respectively, of copending Application No. 10/636,283 (published as US Patent Application Publication 2004/0049678). This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

The Examiner notes that, although the claims of the present application and those of Application No. 10/636,283 are not identical, they are still considered to claim the same invention. The sole substantive difference is between the "second number" recited in Claims 1 and 11 of the '283 application and the "random number encrypted using the second key" in Claims 1, 6, and 11 of the present application; however, the steps of generating the "second number" in the claims of the '283 application are identical to those that result in the "random number encrypted using the second key" in

the claims of the present application. It appears that the two limitations are thus defined so as to be interchangeable, and therefore the claims are directed to the same invention.

8. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

9. Claims 1, 2, 5-10, 12-14, and 16-20 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 2, 3, 5-10, and 12-20 of copending Application No. 10/203,559. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claim 3 of the '559 application contains every element of Claim 1 of the present application and, as such, anticipates Claim 1 of the present application. "A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or

anticipated by, the earlier claim. *In re Longi*, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); *In re Berg*, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus)." *Eli Lilly and Co. v. Barr Laboratories, Inc.*, 58 USPQ2d 1869, 1878 (CAFC 2001). Claims 2, 5-10, 12-14, and 16-20 (of the present application) depend from provisionally rejected Claims 1 and 11 and recite the same limitations as Claims 2, 5-10, 12-14, and 16-20 of the '559 application; it would be obvious to include the limitations present in the dependent claims in both the instant application and the '559 application.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

10. Claims 1, 2, 4, 5, 7-10, 12-14, and 16-20 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 2-5, 7-10, and 12-20 of copending Application No. 10/636,283. Although the conflicting claims are not identical, they are not patentably distinct from each other because Claim 3 of the '559 application contains every element of Claim 1 of the present application and, as such, anticipates Claim 1 of the present application. See above for further detail. Claims 2, 4, 5, 7-10, 12-14, and 16-20 (of the present application) depend from provisionally rejected Claims 1 and 11 and recite the same limitations as Claims 2, 4, 5, 7-10, 12-14, and 16-20 of the '283 application; it would be obvious to include the

limitations present in the dependent claims in both the instant application and the '283 application.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

11. Claims 1, 2, 4-14, and 16-20 of this application conflict with claims 1-3 and 5-20 of Application No. 10/203,559. Claims 1, 2, 4-14, and 16-20 of this application also conflict with claims 1-5 and 7-20 of Application No. 10/636,283. 37 CFR 1.78(b) provides that when two or more applications filed by the same applicant contain conflicting claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

***Claim Rejections - 35 USC § 103***

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1, 2, 4, 6-14, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Spies et al, US Patent 5689565.

In reference to Claim 1, Sony discloses an authentication method (see Figures 7-9, Claim 1, and column 2, line 49-column 3, line 17) in which a random number is generated by a random function (column 8, lines 12-17) and encrypted with a symmetric encryption function using a first key in a first apparatus (column 9, lines 13-17). The encrypted random number is sent to a second apparatus (column 9, lines 18-21) and decrypted with a symmetric decryption function using the first key (column 9, lines 31-37), and then encrypted with the symmetric encryption function using a second key (column 9, lines 41-48) and sent to the first apparatus (column 9, line 57-column 10, line 2). The encrypted random number is compared with the originally encrypted random number (column 10, lines 29-31) after first being decrypted with the symmetric decryption function using the second key (column 10, lines 21-28). The two numbers matching authenticates the second apparatus (column 10, lines 31-35) and the two numbers not matching does not authenticate the second apparatus (column 10, lines 36-39). However, Sony does not disclose the calculation and comparison of a digital signature as a step of the authentication method.

Spies discloses a cryptographic system and method that includes generating a digital signature of a document (column 12, lines 6-13) and encrypting the document and digital signature under the same symmetric encryption key in a sending device (column 12, lines 14-27, noting especially the equation at line 25). Spies further

discloses decrypting the document and signature at a receiving device (column 13, lines 15-22) and verifying the signature (column 13, lines 20-36). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Sony by including the steps of generating a digital signature of the random number (the "document") and encrypting the signature with the random number in the first apparatus, and of decrypting and verifying the signature in the second apparatus, in order to authenticate the sending of the random number (see Spies, column 13, lines 26-32) and more generally to allow for greater security, privacy, authenticity, and integrity in the system (see Spies, column 2, lines 1-4).

Further, Sony and Spies are silent as to how the random function generates the random number; however, Official notice is taken that it is well known in the art to use a random function that uses a seed to generate random numbers, for example, a linear feedback shift register or other function taking a seed. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Sony and Spies to include the use of a random function with a seed, in order to gain the well-known benefits of a cryptographically secure (pseudo-)random number generator.

In reference to Claim 2, Sony and Spies further disclose that the first and second keys are held in both the first and second apparatuses (see Sony, Figure 9).

In reference to Claim 4, Sony and Spies further disclose that the second apparatus holds a decryption function (see Sony, column 9, lines 31-37).

In reference to Claim 6, Sony and Spies further disclose that the second apparatus decrypts the random number with the first key (see Sony, column 9, lines 31-37), encrypts the random number with the second key (Sony, column 9, lines 41-48), and sends the encrypted random number to the first apparatus (Sony, column 9, line 57-column 10, line 2). Additionally, Sony and Spies further disclose verifying the signature in the second apparatus (see Spies, column 13, lines 20-36).

In reference to Claim 7, Sony and Spies further disclose that the second apparatus monitors the time elapsed between steps of its processing (see Sony, column 10, lines 53-56).

In reference to Claim 8, Sony and Spies further disclose that the function generating the random numbers is held in the first apparatus (see Sony, column 8, lines 12-15). Additionally, Sony and Spies disclose that if the second apparatus is not authenticated, the authentication process is terminated (Sony, column 10, lines 36-39).

In reference to Claim 9, Sony and Spies further disclose that the first apparatus monitors the time elapsed between steps of its processing (see Sony, column 10, lines 6-7).

In reference to Claim 10, Sony and Spies further disclose that it is determined if the second apparatus is valid (see Sony, column 10, lines 31-35) or not (Sony, column 10, lines 36-39).

Claims 11-14 and 17-20 are system claims reciting limitations corresponding substantially to those of the methods of Claims 1, 2, 4, and 6-10, and are thus rejected by a similar rationale.

14. Claims 5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony in view of Spies as applied to claims 1 and 11 above, and further in view of Schneier, *Applied Cryptography*.

Sony as modified by Spies discloses everything as applied to Claims 1 and 11 above. However, Sony does not disclose the use of digital signatures, and Spies does not explicitly disclose the use of digital signatures of 160 bits. Schneier discloses that hash functions can be used in the creation of digital signatures, and specifically discloses the use of 160 bit hashes (page 38, last paragraph). Therefore, it would have been obvious to modify the method of Sony and Spies to include digital signatures 160 bits in length in order to increase the speed of the signature algorithm (see Schneier, page 38, last paragraph-page 39, first full paragraph).

## ***Conclusion***

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Messing, US Patent 7039805, discloses a digital signature where the digital signature (created by asymmetric techniques) is further encrypted by a symmetric encryption algorithm.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER